

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-344094

(43)Date of publication of application : 14.12.2001

(51)Int.Cl.

G06F 7/58

H03K 3/84

(21)Application number : 2000-163184

(71)Applicant : NTT ELECTRONICS CORP

(22)Date of filing : 31.05.2000

(72)Inventor : ISHII HARUHIKO

TANAKA YUKIO

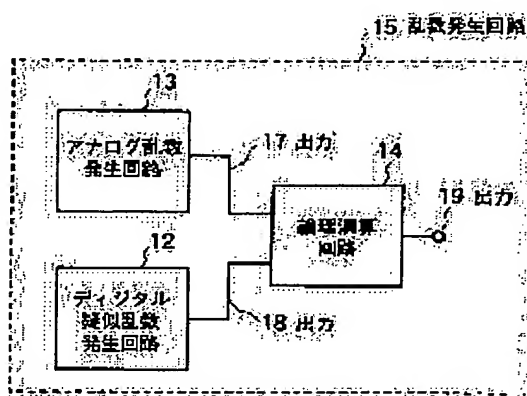
KAMIYAMA KENICHI

(54) CIRCUIT FOR GENERATING RANDOM NUMBER

(57)Abstract:

PROBLEM TO BE SOLVED: To realize a random number generating circuit in which the generation frequency of random numbers can be made uniform, and reproducibility can be prevented from being generated.

SOLUTION: This circuit is provided with an analog random number generating circuit 13 for amplifying a noise generated like an analog from the fluctuation of currents running through electronic components such as a resistance or a semiconductor element, and for outputting it as random numbers, a digital pseudo random number generating circuit 12 for generating and outputting digital pseudo random numbers according to the combination of a register and a logical arithmetic element or a software arithmetic operation, and a logical arithmetic circuit 14 for performing the logical arithmetic operation of the output of the analog random number generating circuit 13 and the output of the digital pseudo random number generating circuit 12, and outputting the arithmetic result.



LEGAL STATUS

[Date of request for examination] 12.12.2000

[Date of sending the examiner's decision of rejection] 15.06.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁(JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2001-344094

(P 2001-344094A)

(43) 公開日 平成13年12月14日 (2001. 12. 14)

(51) Int. Cl. 7

識別記号

F I

テーマコード (参考)

G 0 6 F 7/58

G 0 6 F 7/58

A 5J049

H 0 3 K 3/84

H 0 3 K 3/84

Z

審査請求 有 請求項の数 2 O L

(全 4 頁)

(21) 出願番号 特願2000-163184 (P2000-163184)

(22) 出願日 平成12年5月31日 (2000. 5. 31)

(71) 出願人 591230295

エヌティティエレクトロニクス株式会社
東京都渋谷区道玄坂1丁目12番1号

(72) 発明者 石井 春彦

東京都渋谷区道玄坂1-12-1 エヌティティ
エレクトロニクス株式会社内

(72) 発明者 田中 幸男

東京都渋谷区道玄坂1-12-1 エヌティティ
エレクトロニクス株式会社内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外5名)

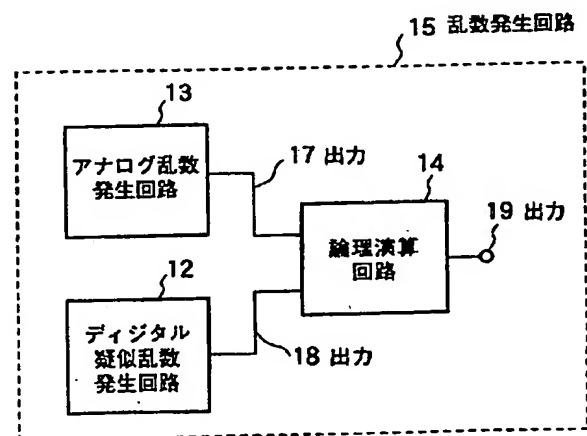
最終頁に続く

(54) 【発明の名称】 乱数発生回路

(57) 【要約】

【課題】 本発明の課題は、発生頻度が一定でかつ再現性の無い乱数発生回路を簡易な構成で実現することにある。

【解決手段】 本発明は、抵抗や半導体素子等の電子部品に流れる電流の揺らぎからアナログ的に発生する雑音を増幅して乱数として出力するアナログ乱数発生回路13と、レジスタと論理演算素子の組合せあるいはソフトウェア演算によりデジタル疑似乱数を発生し出力するデジタル疑似乱数発生回路12と、該アナログ乱数発生回路13の出力と該デジタル疑似乱数発生回路12の出力とを論理演算して出力する論理演算回路14とを具備することを特徴とするものである。



【特許請求の範囲】

【請求項 1】 抵抗や半導体素子等の電子部品に流れる電流の揺らぎからアナログ的に発生する雑音を増幅して乱数として出力するアナログ乱数発生回路と、レジスタと論理演算素子の組合せあるいはソフトウェア演算によりデジタル疑似乱数を発生し出力するデジタル疑似乱数発生回路と、

該アナログ乱数発生回路の出力と該デジタル疑似乱数発生回路の出力とを論理演算して出力する論理演算回路とを具備することを特徴とする乱数発生回路。

【請求項 2】 アナログ乱数発生回路として、相補形の 2 個のトランジスタペアの入力端子どうし及び出力端子どうしを接続したインバータと該インバータの入力端子と出力端子との間に接続された帰還抵抗とで構成されたインバータアンプをコンデンサを介在することにより複数段交流的に結合して初段のインバータアンプで発生したアナログ的雑音を増幅し乱数として出力するアナログ乱数発生回路を用いることを特徴とする請求項 1 記載の乱数発生回路。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は 2 値 (1/0) の乱数を時系列的に発生させる乱数発生回路に関する。

【0002】

【従来の技術】 近年、クレジットカードなどで使用されている磁気カードの偽造防止対策として、暗号回路を搭載した IC カードの開発が進められている。セキュリティを高めるためには暗号回路内に発生頻度が一樣でかつ再現性のない乱数を発生させる回路が必要である。

【0003】 従来、乱数 (= 雑音) を発生させる方法としては、レジスタと論理回路の組合せにより疑似乱数を発生させる方法と、抵抗や半導体素子等に流れる電流の揺らぎに伴う雑音を増幅して 2 値乱数データを得る方法が多く用いられてきた。

【0004】 前者の代表例としては M 系列符号がある。図 2 は 7 段の M 系列発生回路 21 の構成例を示す。22 は 7 段のシフトレジスタであり、その 4 段目出力 23 と 7 段目出力 24 を入力とする排他的論理和回路 (XOR) 25 の出力を 1 段目の入力に帰還しており、クロック 26 の立上り毎に各段のシフトレジスタ 22 のデータが右へ 1 ビットずつシフトされることにより、7 段目の出力 24 から 2 値の乱数が出力される。

【0005】 そのシリアル出力を 7 ビット毎に区切って数値化したデータ (1~127) の発生頻度は図 3 の乱数出力 31 に示すように完全に均一化されており、偏りの無い理想的な乱数列を出力することができる。

【0006】 しかしながらこの方法では、アルゴリズムと初期値がわかると全く同じ乱数列が再現できるという大きな欠点があった。

【0007】 後者の例としては図 4 に示すようにツェナ

ードダイオード 41 に抵抗 42 を介して電圧源 43 から電流を流し、その両端に発生する雑音を増幅器 44 で電源電圧まで増幅して出力 45 に 2 値の雑音 (= 乱数) を出力する方法がある。この方法では、電流の偶然の揺らぎを利用して雑音を発生するため、前者のように全く同じ雑音 (= 乱数) が再現されるおそれは無いが、出力データの発生頻度は図 5 の乱数出力 51 に示すように必ずしも均一なものが得られるとは限らず、出力されないデータ出力値も見られる。従来のこの方法では、精度の良い乱数を発生させることが困難という欠点があった。また、回路を LSI 化する場合、通常多く使用される CMOS プロセスではツェナードダイオードが容易に作成できないという欠点もあった。

【0008】

【発明が解決しようとする課題】 本発明は上記の事情に鑑みてなされたもので、発生頻度が一樣で再現性の無い乱数を発生させる乱数発生回路を提供することを目的とする。

【0009】

20 【課題を解決するための手段】 上記目的を達成するために本発明の乱数発生回路は、抵抗や半導体素子等の電子部品に流れる電流の揺らぎからアナログ的に発生する雑音を増幅して乱数として出力するアナログ乱数発生回路と、レジスタと論理演算素子の組合せあるいはソフトウェア演算によりデジタル疑似乱数を発生し出力するデジタル疑似乱数発生回路と、該アナログ乱数発生回路の出力と該デジタル疑似乱数発生回路の出力とを論理演算して出力する論理演算回路とを具備することを特徴とするものである。

30 【0010】 また本発明は、前記乱数発生回路において、アナログ乱数発生回路として、相補形の 2 個のトランジスタペアの入力端子どうし及び出力端子どうしを接続したインバータと該インバータの入力端子と出力端子との間に接続された帰還抵抗とで構成されたインバータアンプをコンデンサを介在することにより複数段交流的に結合して初段のインバータアンプで発生したアナログ的雑音を増幅し乱数として出力するアナログ乱数発生回路を用いることを特徴とするものである。

40 【0011】 本発明による乱数発生回路は、デジタル疑似乱数発生回路とアナログ乱数発生回路との出力どうしの論理演算をとることにより、上記の問題を解決するものである。

【0012】 即ち、均一性が不十分なアナログ的乱数を、再現されるおそれはあるが均一性の高いデジタル疑似乱数と論理演算することにより、スペクトラムを拡散し、再現性がなくかつ均一性が確保できる乱数を発生することを特徴とする。

【0013】

【発明の実施の形態】 以下図面を参照して本発明の実施形態例を詳細に説明する。

【0014】本発明の一実施形態例を図1に示す。乱数発生回路15はデジタル疑似乱数発生回路12、アナログ乱数発生回路13、及び論理演算回路14より構成される。デジタル疑似乱数発生回路12は例えば図2に示すようなM系列符号等、デジタル的に疑似乱数を発生させる回路であり、公知の技術で容易に実現できるものである。デジタル疑似乱数発生回路12の出力18からは均一性の良いシリアル乱数データが出力される。アナログ乱数発生回路13は電流の揺らぎ等、アナログ的な発生源から乱数（＝雑音）を発生させる回路であり、例えば図4に示すようなツェナーダイオードを利用した方法等の公知の従来技術でも実現できる。

【0015】本発明による他の実施形態例としては、図6に示すようなインバータアンプを多段接続したアナログ乱数発生回路60の構成によるものが使用可能である。

【0016】603はインバータ素子であり、相補形の2個のトランジスタペアの入力端子どうし及び出力端子どうしを接続して構成される。例えばCMOS-LSIプロセスではnチャネルトランジスタとpチャネルトランジスタ各1個の組合せで容易に実現できる。このインバータ素子603の入・出力端子間に抵抗604により負帰還をかけることにより、簡易な構成でアナログのインバータアンプ61が実現できる。インバータアンプ61の出力601には、内部トランジスタに流れる電流の揺らぎによる微小な雑音が発生し、コンデンサ602により交流的に結合された次段のインバータアンプ61により増幅される。多段接続のインバータアンプ61により電源電圧まで増幅された雑音振幅が出力バッファ回路62により、2値のデジタル雑音信号に変換され、出力603にシリアルで乱数として出力される。

【0017】出力バッファ回路62は通常CMOSプロセスで多く用いられるデジタルインバータ素子等で容易に実現可能である。

【0018】図1に示す乱数発生回路15内の論理演算回路14はアナログ乱数発生回路13の出力17とデジタル疑似乱数発生回路12の出力18を入力として論理演算を行い出力19を生じる回路である。論理演算回路14の簡単な例としては排他的論理和（XOR）回路等が適用可能であるが、他のより複雑な論理回路であっても良い。

【0019】論理演算回路14により論理演算された乱数出力の発生頻度例を図7に示す。乱数出力71は、図3のM系列符号と比較すると発生頻度には多少ばらつきが見られるものの、図5のアナログ乱数発生回路のような出力されないデータ出力値は見られず、大きな改善効果が見られる。

【0020】

【発明の効果】以上説明したように本発明によれば、アナログ乱数発生回路により発生された再現性は無いが一

様性が十分でない乱数と、デジタル疑似乱数発生回路により発生された一様性は十分だが、再現性のある乱数とを論理演算することにより、両者の長所のみを取り出した一様性があり、再現性の無い乱数を容易に得ることができる。

【0021】また、アナログ乱数発生回路については、インバータアンプを交流結合により複数段シリーズに接続することにより、LSI化が容易になるという利点がある。

【0022】なお、以上の説明ではデジタル疑似乱数発生回路は7段のM系列符号をハードウェアで発生する場合を例にとって説明したが、段数はこれ以外でもよく、また符号の種類もM系列以外のものでもよい。またマイクロプロセッサ等のソフトウェアで演算して実現する方法であってもよい。

【図面の簡単な説明】

【図1】本発明に係る乱数発生回路の一実施形態例を示す構成説明図である。

【図2】従来のデジタル疑似乱数発生回路の一例を示す回路図である。

【図3】図2のデジタル疑似乱数発生回路のデータ出力値に対する発生頻度の一例を示す特性図である。

【図4】従来のアナログ乱数発生回路の一例を示す回路図である。

【図5】図4のアナログ乱数発生回路のデータ出力値に対する発生頻度の一例を示す特性図である。

【図6】本発明に係るアナログ乱数発生回路の一例を示す回路図である。

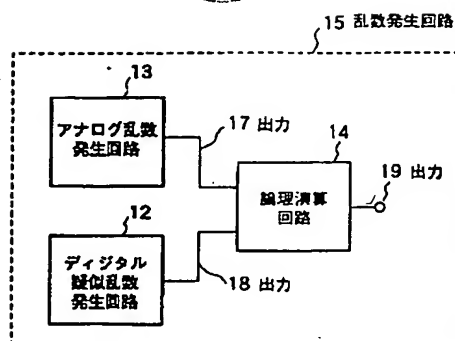
【図7】本発明に係る乱数発生回路のデータ出力値に対する発生頻度の一例を示す特性図である。

【符号の説明】

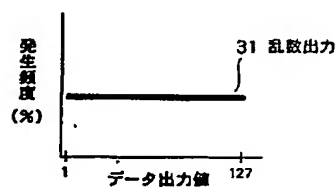
12 デジタル疑似乱数発生回路
13, 60 アナログ乱数発生回路
14 論理演算回路
15 乱数発生回路
17, 18, 19, 45, 63, 601 出力
21 M系列発生回路
22 シフトレジスタ
23 4段目出力
24 7段目出力
25 排他的論理和回路（XOR）
26 クロック
31, 51, 71 乱数出力
41 ツェナーダイオード
42, 604 抵抗
43 電圧源
44 増幅器
61 インバータアンプ
62 出力バッファ回路
602 コンデンサ

603 インバータ素子

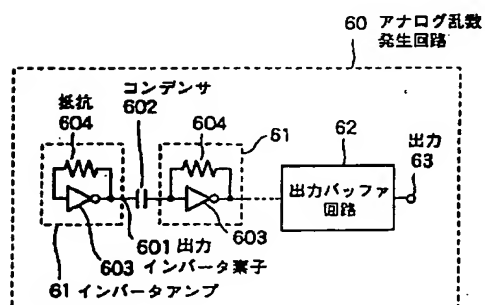
【図1】



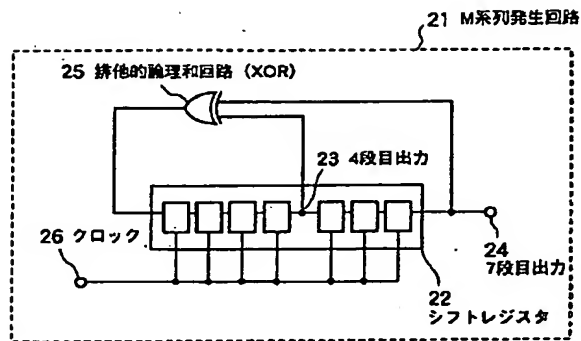
【図3】



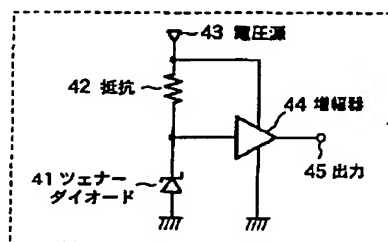
【図6】



【図2】



【図4】



【図7】



フロントページの続き

(72)発明者 神山 健一

東京都渋谷区道玄坂1-12-1 エヌティ
ティエレクトロニクス株式会社内

Fターム(参考) 5J049 CA03 CA09 CA10